

Claims

- Sub
A 26
1. A device for communicating with other devices to allow them to access applications, comprising:
- 5 at least a first application;
- authentication means for authenticating a communicating device;
- access control means accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether
- 10 access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device.
- 15 2. A device as claimed in claim 1 wherein the access control means is arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration.
- 20 3. A device as claimed in claim 1 further comprising a user interface for authorising access to an application during arbitration, the access control means being arranged to store security indications in association with accessible applications, wherein the stored security indication associated with
- 25 the first application is indicative of whether user authorisation of the communicating device is or is not required during arbitration.
4. A device as claimed in claim 2 wherein the stored security indication associated with the first application is indicative of whether authentication of

5. A device as claimed in claim 3 wherein the access control means is further arranged to store trust indications in association with devices, and wherein the stored security indication associated with the first application is indicative of whether user authorisation of the communicating device is or is not required during arbitration in dependence upon any stored trust indication associated with the communicating device.

6. A device as claimed in claim 1 further comprising a user interface for authorising access to an application during arbitration, the access control means being arranged to store trust indications in association with devices, wherein if there is a stored trust indication associated with the communicating device then no user authorisation is required.

7. A device as claimed in claim 6 wherein the access control means receives indications originating from communicating device identifying the communicating device.

8. A device as claimed in claim 1 further comprising a user interface for authorising access to an application during arbitration, the access control means being arranged to store trust indications in association with devices and to store security indications in association with accessible applications, wherein if there is a stored trust indication associated with the communicating device then no user authorisation is required and if there is no trust indication associated with the communicating device user authorisation is required in dependence on the stored security indication associated with the requested application.

30

9. A device as claimed in claim 5 wherein the access control means receives indications originating from the communicating device identifying the communicating device and the application requested.

5 10. A device as claimed in claim 1 having a device database which stores trust indications of different devices.

11. A device as claimed in claim 1 having a service database for storing security indications of the accessible applications.

10

12 A device as claimed in claim 1 wherein authentication comprises secret key exchange between the device and the communicating device.

15

13. A device as claimed in claim 1 wherein the access control means is an/the interface with the first application.

20

14. A device as claimed in claim 1 having a protocol stack comprising a first layer and a second higher layer overlying the first layer, with or without, intermediary layers, wherein the first lower layer is the authentication means and the second higher layer is part of the access control means.

15. A device as claimed in claim 14 wherein the second layer in combination with a security manager is the access control means.

25

16. A device as claimed in claim 14 wherein the first layer is the Link Manager Protocol Layer according to the presently proposed Bluetooth specification v0.9 or its equivalent.

009090" E0088560

17. A device as claimed in claim 14 wherein the second layer is not the Link Manager Protocol Layer according to the presently proposed Bluetooth specification v0.9 or its equivalent.

5 18. A device as claimed in claim 1 comprising a plurality of applications and a plurality of access control means where each application has an access control means connected to it.

10 19. A device as claimed in claim 18 wherein the plurality of access control means are arranged in a hierarchy, wherein a first access control means at the lowest level in the hierarchy provides access to at least a second access control means and access to one or both of a third access control means and an application, wherein access to each application is provided via one or more access control means including the first access control means and the
15 application's connected access control means, if different, and wherein any access control means is accessible by a communicating device requesting access to one of its connected applications without the communicating device having been authenticated by the authentication means, and is arranged to arbitrate whether access of the communicating device to the one connected
20 application is granted or refused, the connected access control means instructing the authentication means to authenticate the communicating device if the arbitration requires an authentication of the communicating device.

25 20. A device as claimed in claim 14 wherein the or each access control means includes one of a plurality of different multiplexing protocol layers

30 21. A device as claimed in claim 20 wherein each access control means is the combination of the one multiplexing protocol layer and a security manager

5 23. A device as claimed in claim 14 wherein a request to access the first application proceeds up through the protocol stack to the access control means.

25. A device as claimed in claim 15 wherein the security manager controls the authentication means.

25 27. A device for communicating with other devices to allow them to access applications, comprising:

at least first and second applications;
authentication means for authenticating a communicating device;
first access control means accessible by a communicating device requesting
access to the first application without the communicating device having been
30 authenticated by the authentication means, and arranged to arbitrate whether

access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device.

5 second access control means accessible by a communicating device
requesting access to the second application without the communicating
device having been authenticated by the authentication means, and arranged
to arbitrate whether access of the communicating device to the second
application is granted or refused wherein if the arbitration requires an
10 authentication of the communicating device, the access control means
instructs the authentication means to authenticate the communicating device,
wherein the first access control means is accessible by a communicating
device requesting access to the second application without the
communicating device having been authenticated by the authentication
15 means, and is arranged to provide the access of the communicating device to
the second access means.

28. A method of arbitrating the access of a requesting device to a service provided by a providing device comprising:

20 sending a request to access the service from the requesting device to the
providing device;

receiving the request at the providing device and passing it, without authenticating the requesting device, to an arbitration means interfacing the service;

25 determining, in the arbitration means, whether to grant or refuse access to
the first application by the requesting device, wherein if the determination
requires an authentication of the requesting device, the authentication is
performed during that determination and not previously.

29. A method as claimed in claim 28 wherein the determination is made on the basis of the identity of service requested and/or the identity of the requesting device.

- 5 30. A device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom;

- 10 arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication, originating from the other device, identifying the other device, wherein, if the requesting device has a stored trust indication associated therewith no user authorisation is required and if the requesting device has no stored trust indication associated therewith user authorisation is requirable; and
- 15 a user interface for providing user authorisation.

- 20 31. A device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom;

- 25 arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and store security indications in association with provided services and arranged to receive from the interface indications, originating from the other device, identifying the other device and the service requested, wherein, if the requesting device has a stored trust indication associated therewith no
- 30 user authorisation is required and if the requesting device has no stored trust

indication associated therewith user authorisation is required in dependence upon the stored security indication associated with the requested service; and a user interface for providing user authorisation.